

# **EXHIBIT 1**

# Bloatware: What it is + how to spot and remove it

---

 [us.norton.com/blog/online-scams/bloatware](https://us.norton.com/blog/online-scams/bloatware)

Is your new device running slow? Bloatware could be the problem. Follow this guide to learn about different types of bloatware, plus how you can find and remove it.

## ***Bloatware definition***

***Bloatware is unwanted and potentially harmful software preloaded onto new devices.***

When you buy a new device, you expect that your equipment should come with a clean slate. After all, we're usually buying new devices to replace old ones that are no longer up to snuff.

The unfortunate reality, however, is that our new devices are often only in near-mint condition. That's thanks to bloatware — unwanted apps and software that are preinstalled on new devices.

It's not to say that all bloatware is bad. Some, like trialware, you might even appreciate and invest in yourself. Others can pose cybersecurity risks and violate your privacy. Regardless of intent, one universal truth is that bloatware, like any download, slows down our devices. And a slow device is not a device in mint condition.

To help get your new devices running, well, good as new, we're outlining how to remove bloatware from different devices, the cybersecurity downfalls of each type of bloatware, and how to avoid it from the start.

## **What is bloatware?**

---

## Bloatware Explained



Bloatware is **unwanted and potentially harmful software** loaded onto new devices.

Bloatware is unwanted and potentially harmful software preloaded onto new devices. Also known as potentially unwanted applications (PUAs), bloatware is often preinstalled by vendors, manufacturers, or carriers as a form of marketing to put services directly in front of consumers.

Considering some consumers might find value in the pre-downloaded software, bloatware is a subjective term. Other consumers, though, might think of bloatware as a weed, and even resort to calling it crapware.

Essentially, any software, program, or app you did not install on a device yourself can be considered bloatware.

### Why bloatware is a cybersecurity threat

Subjective term aside, one objective truth about bloatware is that it slows down your devices. That's because the more programs that are downloaded on your device, the more computing power is being used, and even if you don't use the bloatware program, it's still taking up

memory on your device.

As a result, your device and the programs you value all run slower. Worse yet, the bloatware might be malicious and downloaded by an unknown party.

To give a real-life example, in 2014 Lenovo preinstalled software called Superfish on its devices to put targeted advertisements in front of consumers. Not only did it result in annoying pop-up ads for users, but Superfish also came with some under-the-radar cybersecurity threats, including vulnerability to serious cybercrimes.

## **How to identify bloatware: 5 warning signs**

---

# Bloatware Warning Signs

5 ways to diagnose whether an app or program is bloatware



There are many types of bloatware, each with its own warning signs. But here a few of the most common red flags to help you identify whether a software, program, or app on your new device is indeed bloatware:

1. **The app or program is hard to uninstall:** In most cases, bloatware is more difficult to remove than regular applications. It may even pop up in your application list after you've deleted it.
2. **You don't recognize the app or program:** If you didn't install the application yourself, it's likely bloatware.
3. **The app or program is persistent about you making purchases:** Certain types of bloatware feature aggressive marketing techniques in which they frequently request payment for access to a paid version of their software.
4. **Your browser has started to display pop-ups:** Bloatware sometimes features annoying pop-up windows that can mess with your browser settings, take you to malicious websites, and even change your homepage.
5. **The app or program is downright useless to you:** A lot of the time, bloatware will be useless to you and other users. They are usually applications you'd never install yourself.

Now that you know how to find bloatware, let's look at the different types of bloatware that can be found on your device.

## **Types of bloatware plus why it's installed**

---

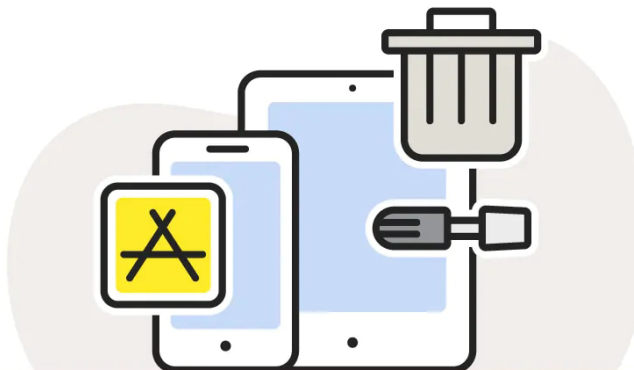
## Bloatware Examples

Some want you to know they're there, while others do not. In either case, these programs can slow down your new device.



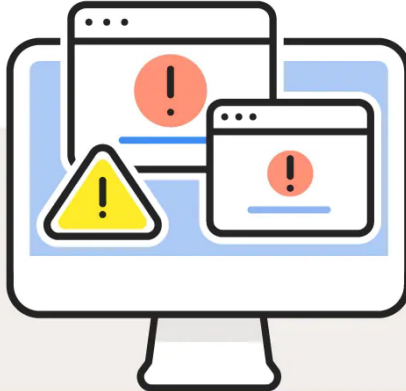
### Trialware

Trialware is trial-based software preinstalled on new devices by third parties who pay manufacturers to put their product in front of consumers.



### Utilities and Applications

Utilities and applications are the bells and whistles pre-downloaded on your new devices, some of which are unremovable because they're required by manufacturers.



## **Adware**

Adware is advertising software installed on new devices to put pop-up advertisements in front of users, as well as potentially malicious downloads.

Generally, bloatware falls into two categories: Software that you know is installed on your devices and software that you don't know is installed on your devices.

The former is often installed by manufacturers, whether that's software manufacturers, device manufacturers, or app developers, to market a product or service to you, perhaps for a trial period. Some developers may even pay manufacturers to install software on devices, and that software could be collecting user data.



So, why do manufacturers allow bloatware to be installed on their devices if it slows them down? It's a revenue stream that offsets retail prices. Turns out, what users don't pay for in the purchase price, they pay for by potentially compromising their privacy and cybersecurity. Not to mention, the headache of dealing with bloatware types that are unremovable.

The second type of bloatware is stealthier because it's purposefully malicious. It's often installed unknowingly even to manufacturers and hidden in software to spy on users. This type of bloatware also can be unknowingly downloaded by users as they're browsing websites and accepting cookies.

Luckily, the more you know, the quicker you can eradicate these pesky and potentially harmful programs.

## **Trialware**

---

As the name indicates, trialware is a trial-based software preinstalled on devices. This form of bloatware is blatantly installed by a third party because they're marketing a service or product to users by giving them a free taste of it. This could even be in the form of antivirus software.

The issues arise when the trial goes away and users no longer wish to use it. The result? The software remains and takes up unnecessary space on a device, weighing down its processing speed. Thankfully, trialware is easy to uninstall on most devices — you just have to remember to do it.

## **Utilities and applications**

---

Of course, every device manufacturer has its own bells and whistles attached to a new device — think stock apps and music apps installed across all Mac and iOS devices.

The problem is when you don't use these preinstalled apps and utilities, they skew more toward junkware and storage hogs. For the most part, third-party applications can be easier to remove, while applications installed by device manufacturers are permanent.

Just consider the following types of bloatware that may come as a “feature” or “add-on” with your devices. And consider if you need them, or if you need to uninstall them.

- Navigation apps
- Browser extensions
- Weather apps
- Games
- Health and fitness apps
- Messaging apps
- Finance apps

- Music players
- Virtual assistants

## Adware

---

Adware is just what it sounds like: advertising software, meaning a piece of software that exists with the sole purpose of putting ads like pop-ups or banner ads in front of users.

It can be the most malicious type of bloatware because the adware can hide in well-intentioned software that developers may even pay manufacturers to install on devices. The reality, however, could be that the adware is capable of spying on users' activity, leaving you vulnerable to cyberattacks. Since adware is hard to detect, it's also harder to eradicate.

## How to get rid of bloatware

---

Some types of bloatware are easy to uninstall, while others require some more effort. Thankfully, there are bloatware removal tools\* that can help you get rid of bloatware. Most are free and some are powered by crowdsourcing to help you determine how detrimental a bloatware program is.

A few popular bloatware uninstallers include:

Part of the equation is also knowing when to uninstall bloatware. Generally, when your device's performance is below par, that's when it's time to turn to one of these tools to scan for bloatware. Of course, bloatware types range across devices, and there are many ways to remove unwanted apps and programs.

Rooting or jailbreaking devices is one way to remove bloatware, as these methods grant users full admin access to remove programs and applications that are even native to devices.

There also are some app removal programs that can root phones for you. We discourage this as this could mean sacrificing your cybersecurity and result in a void of your device's warranty. Advanced users also might want to leverage PowerShell, a scripting language, to clear their devices.

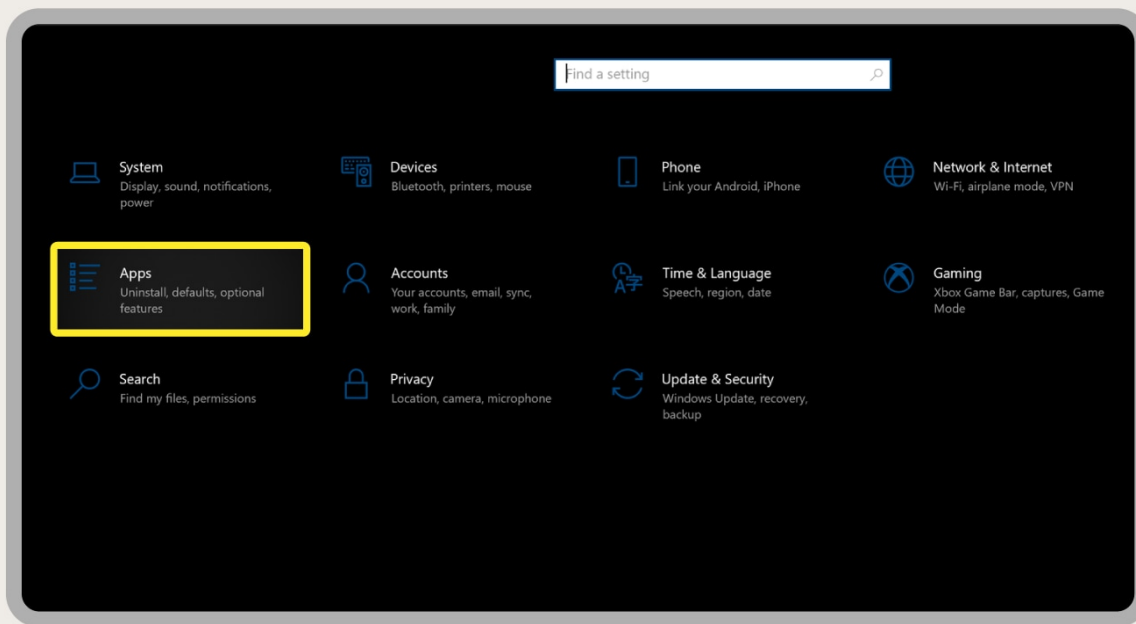
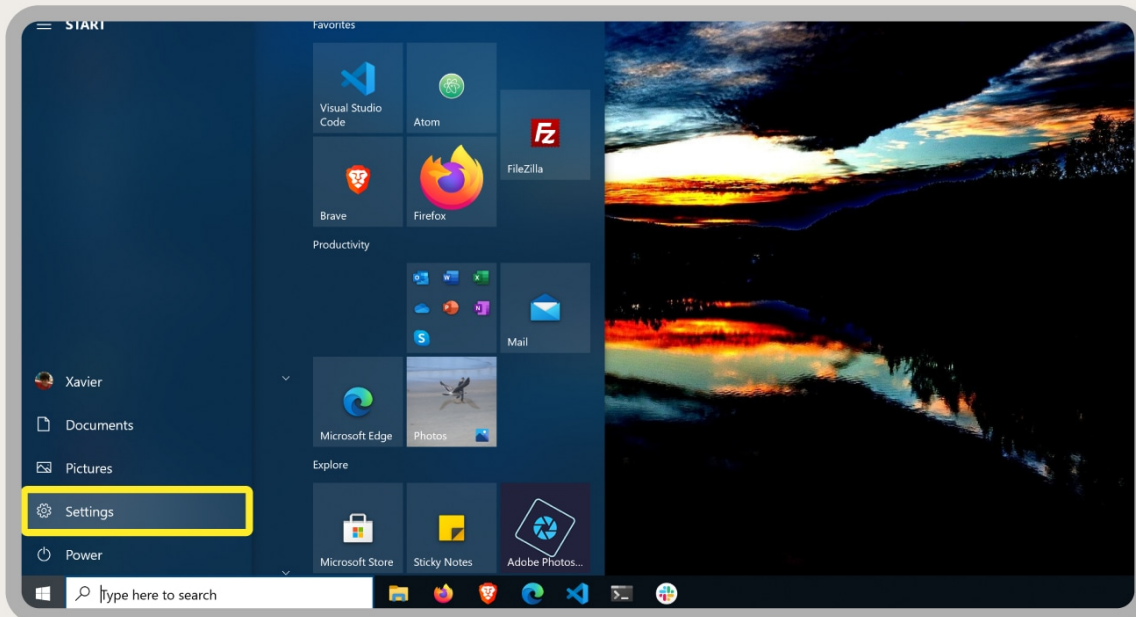
For this piece, **we're overviewing the simplest, safest ways to manually eradicate your devices of bloatware**. In short: We're providing step-by-step instructions for how to delete unwanted apps and programs for common devices.

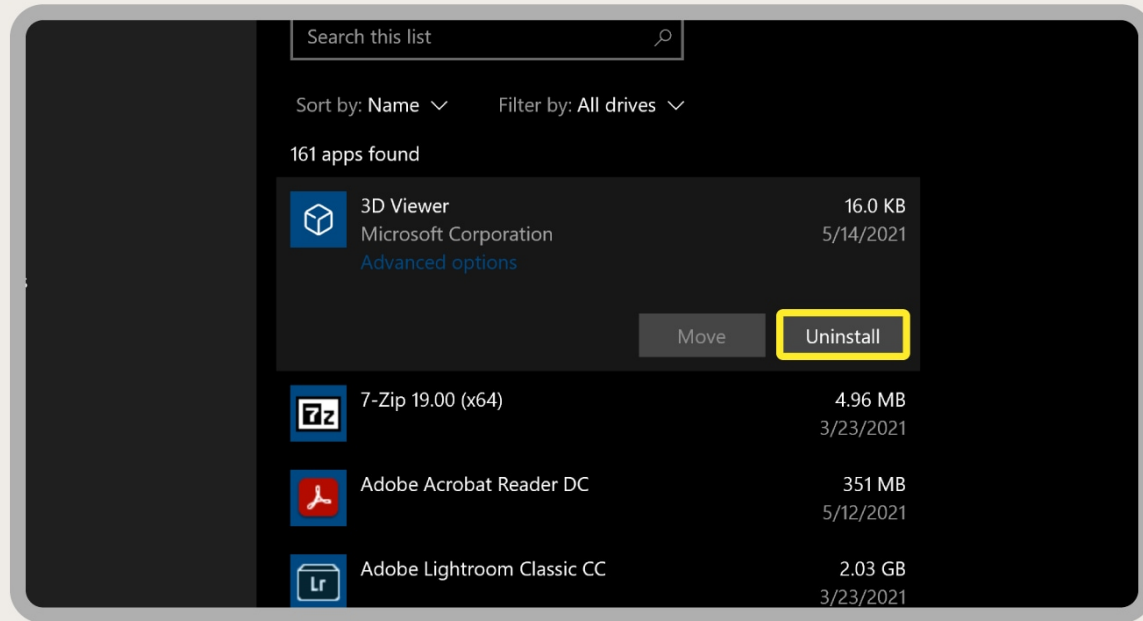
## How to remove bloatware from Windows 10

---

Windows 10 gets a bad rap for having bloatware, but the degree varies depending on the manufacturer. Thankfully, removing unwanted apps and programs is as easy as 1-2-3.

1. From the Start menu, navigate to Settings.
2. In the settings window, click “Apps.”
3. Select the unwanted app (we’re using the preinstalled 3D Viewer as an example) and click “Uninstall.”

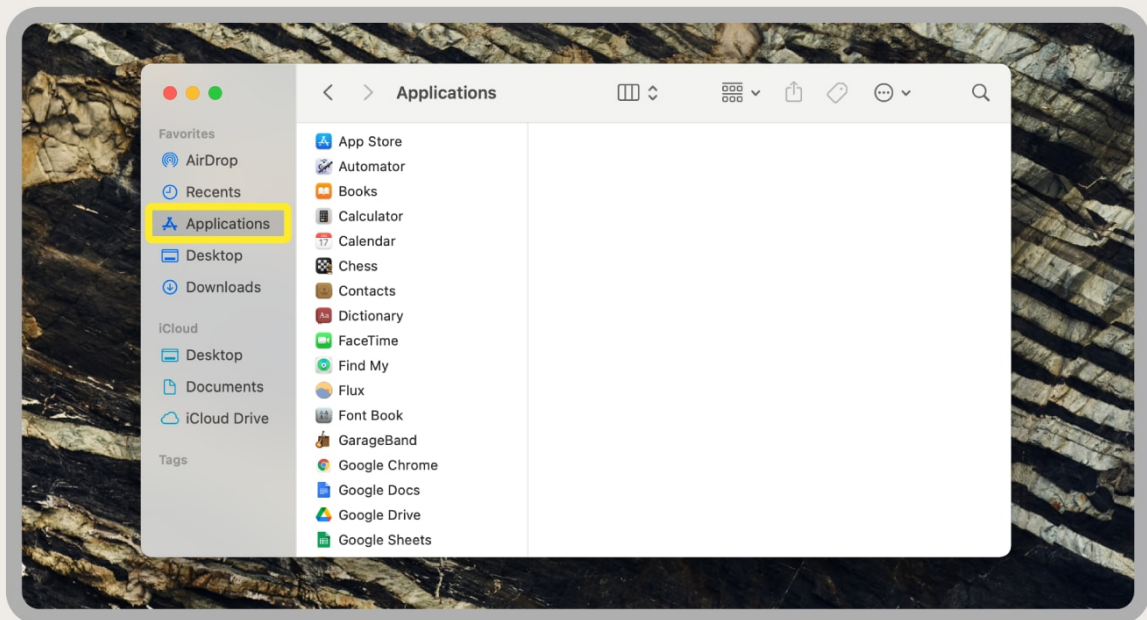




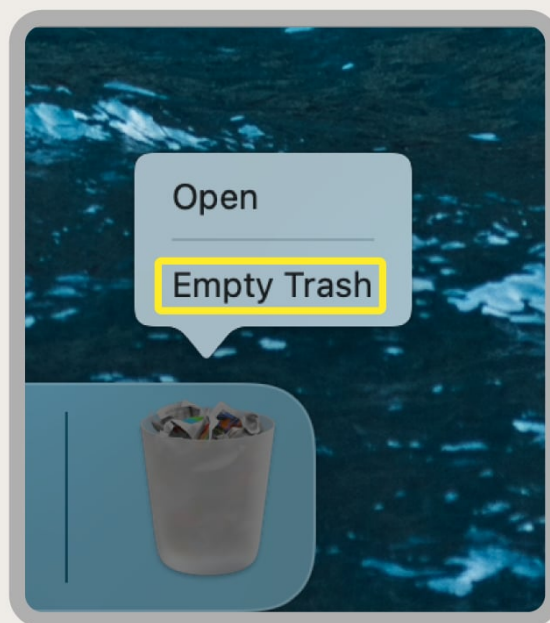
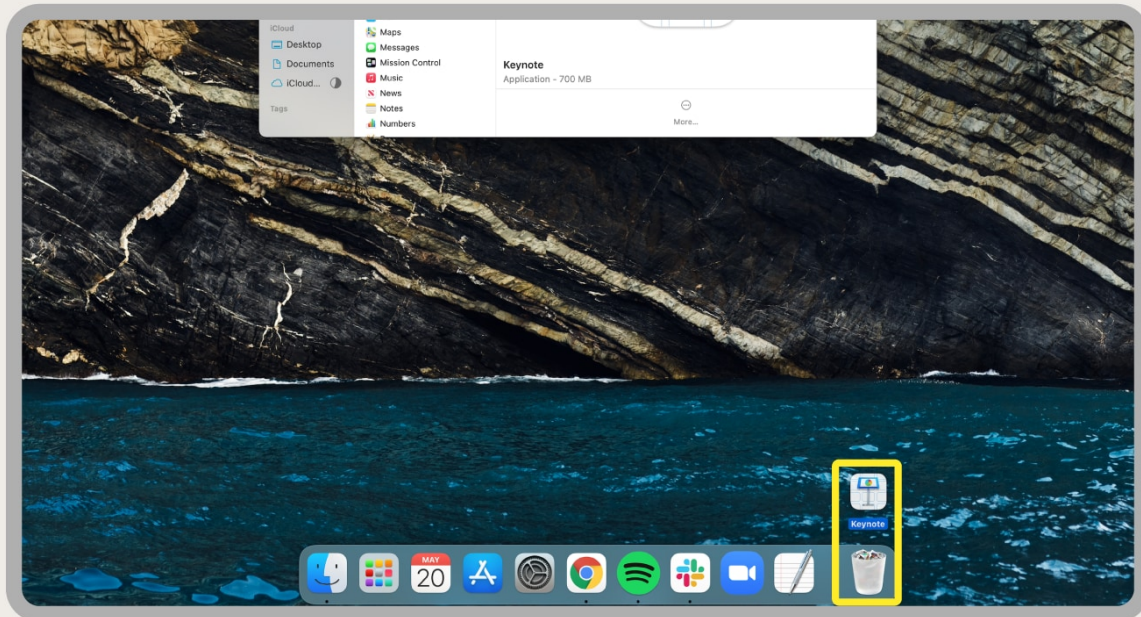
Alternatively, you can use the Windows 10 Refresh Tool, which is essentially a factory reset of your device that removes any downloaded programs. This is perhaps the fastest method to a clean slate, but it's not foolproof, as it could also remove any licensed software you have on your device and won't remove apps or programs that are native to a device.

## How to remove bloatware from MacOS

---







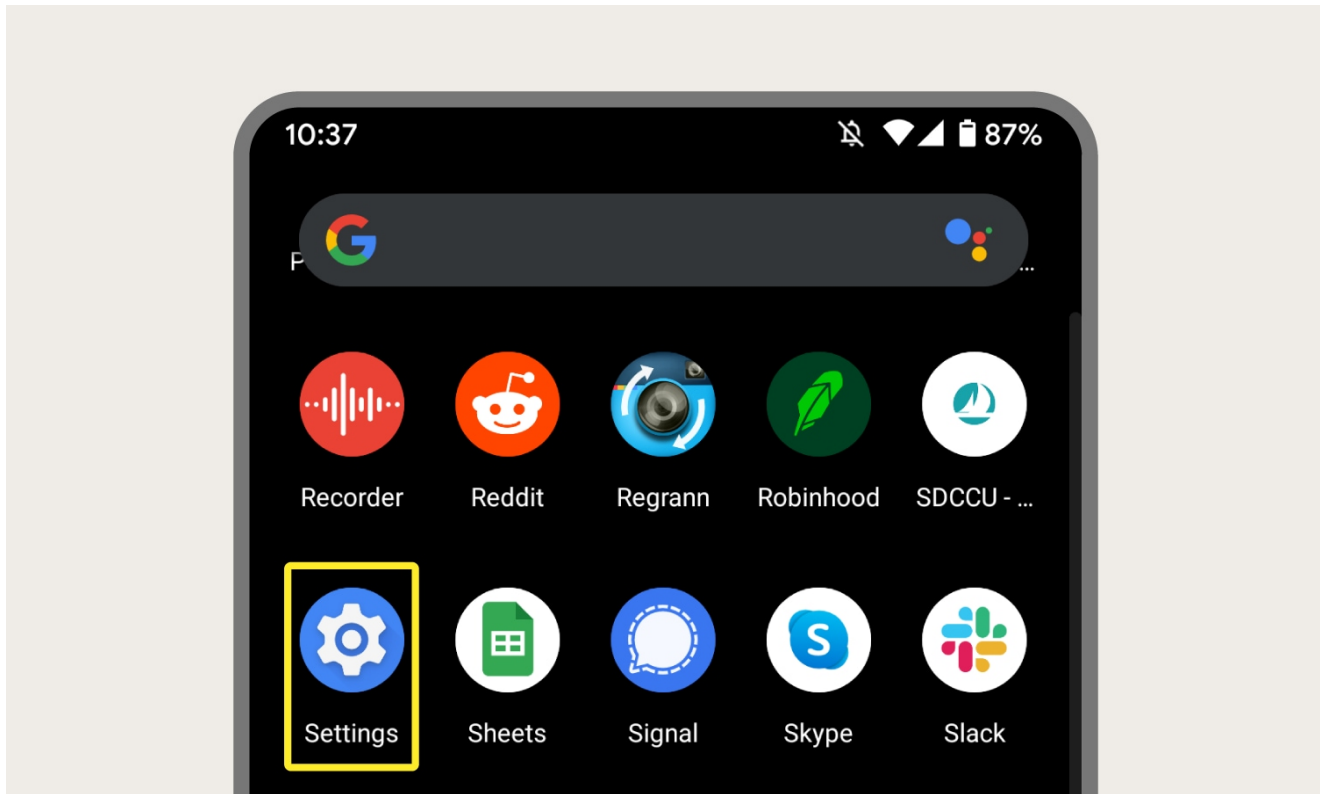
MacOS devices often hold bloatware that stems from our browsing activities, rather than preinstalled software on a new device. This means users should do some regular cleanup of their devices and use the following steps to do so:

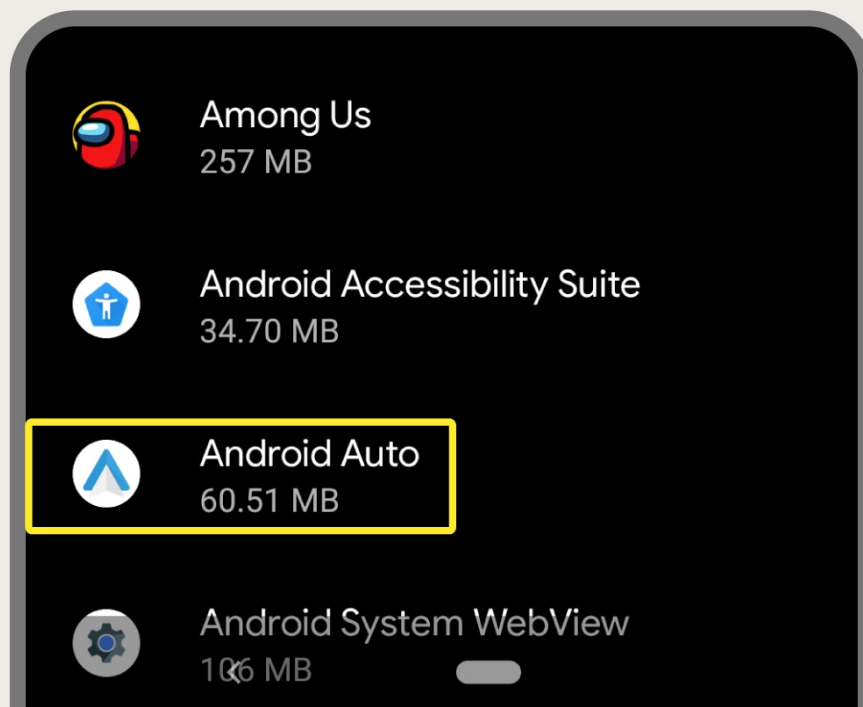
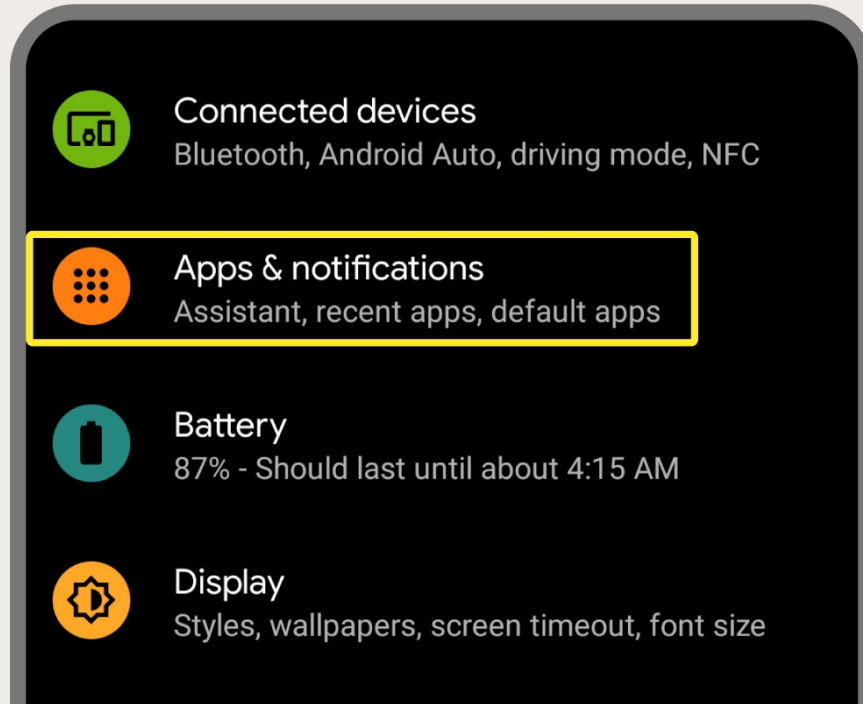
1. Open a new Finder window.

2. Select “Applications” on the left-hand sidebar.
3. Select the unwanted app (we’re using the preinstalled Keynote app as an example) and drag it to your Trash.
4. Right-click your Trash and select “Empty Trash.”

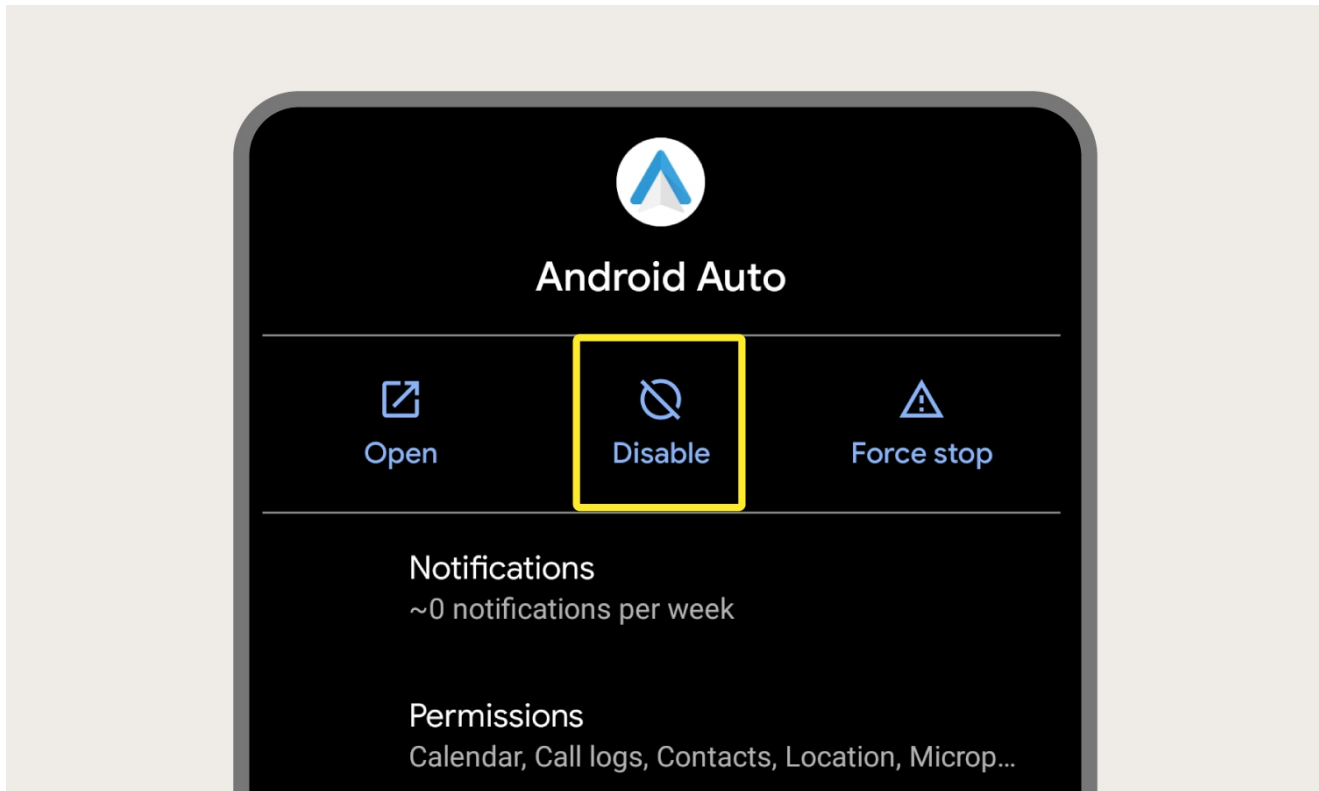
## How to remove bloatware from Android

---







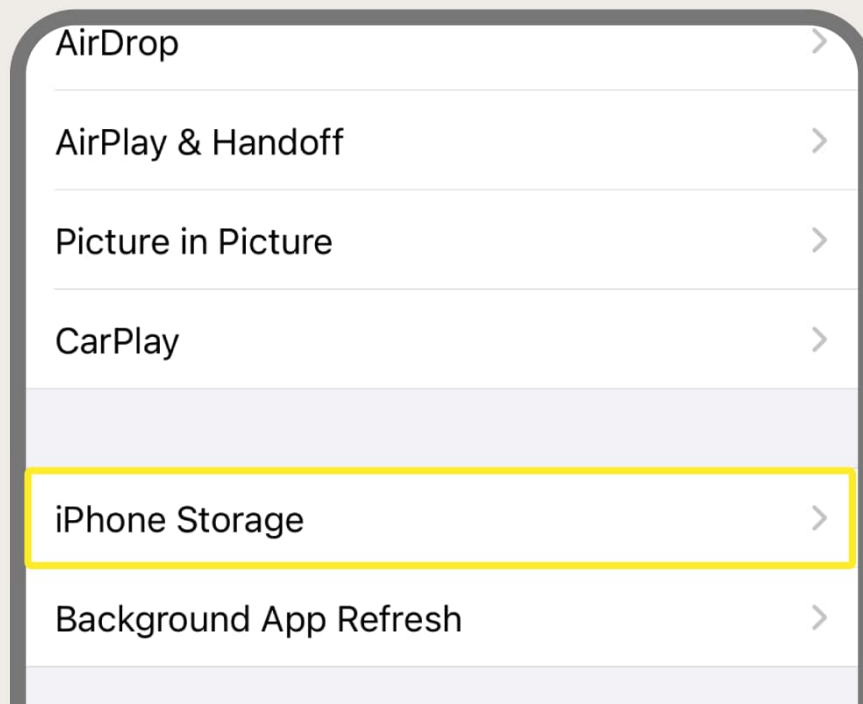
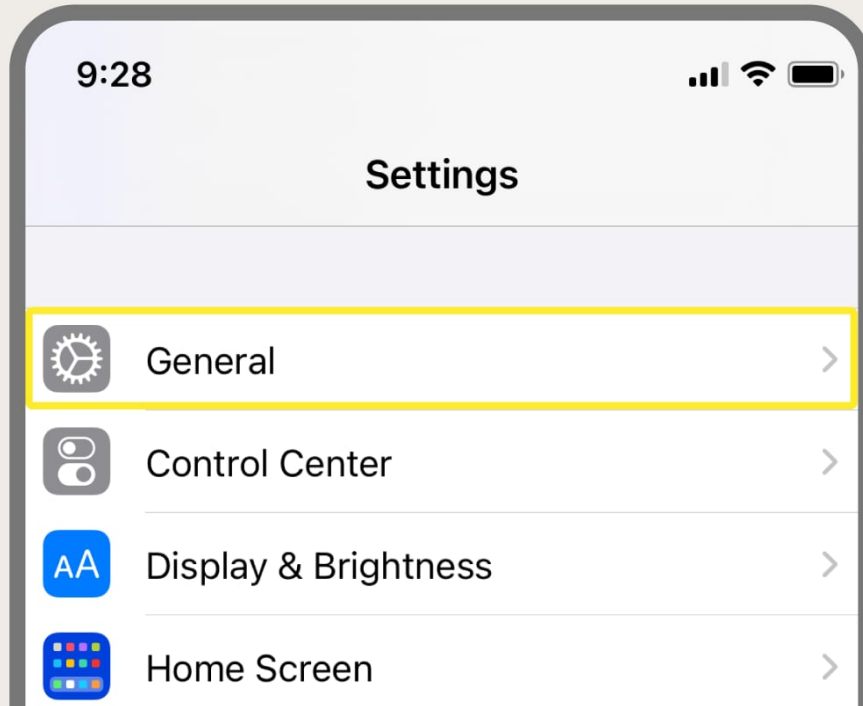


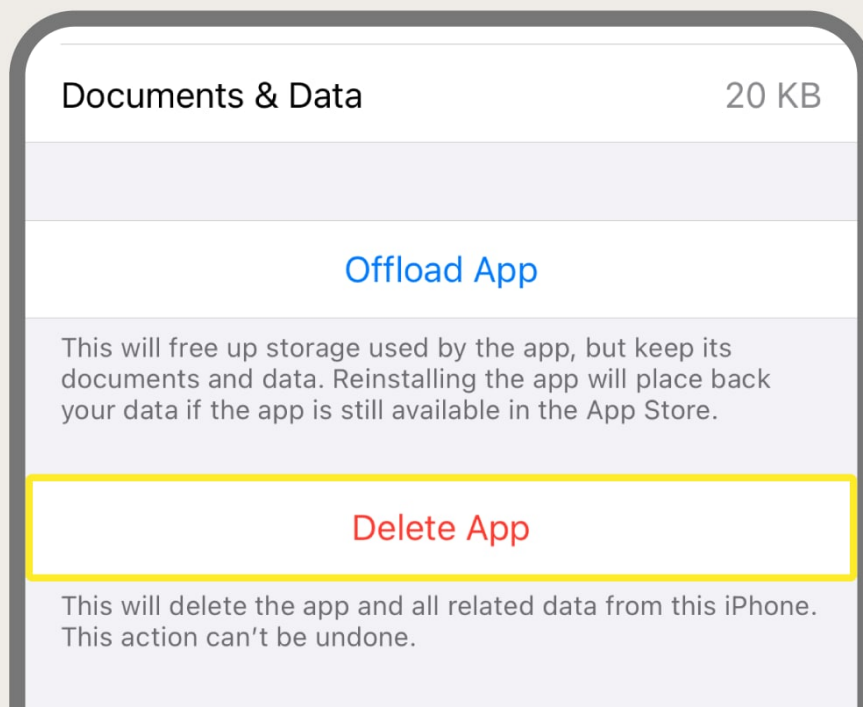
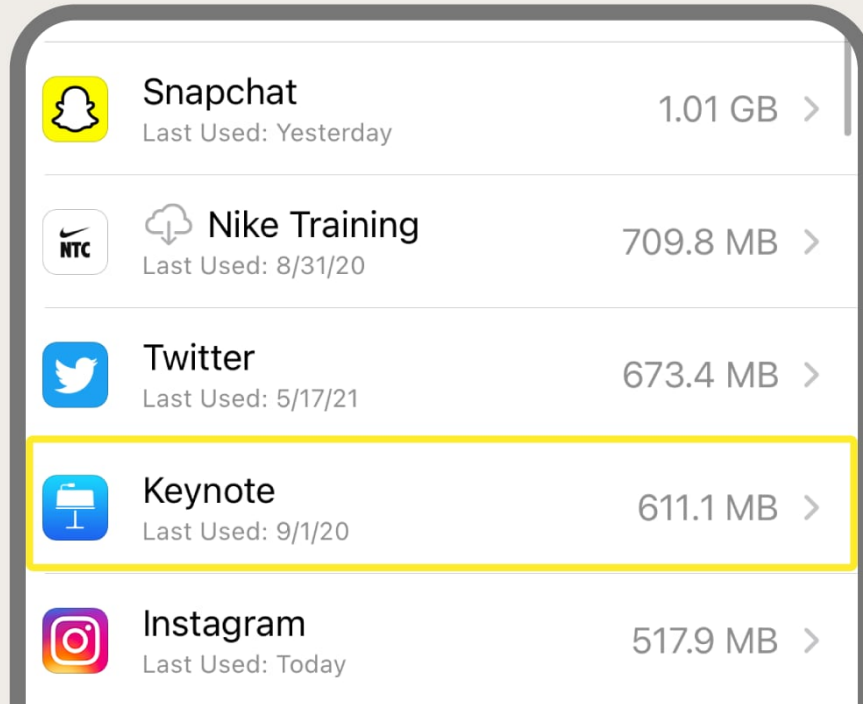
When it comes to Android devices, bloatware often comes in the form of apps. For the safest way to eradicate any on your device, you'll want to disable them. This will ensure the apps don't run in the background of your device, therefore slowing it down, but they will still use storage space.

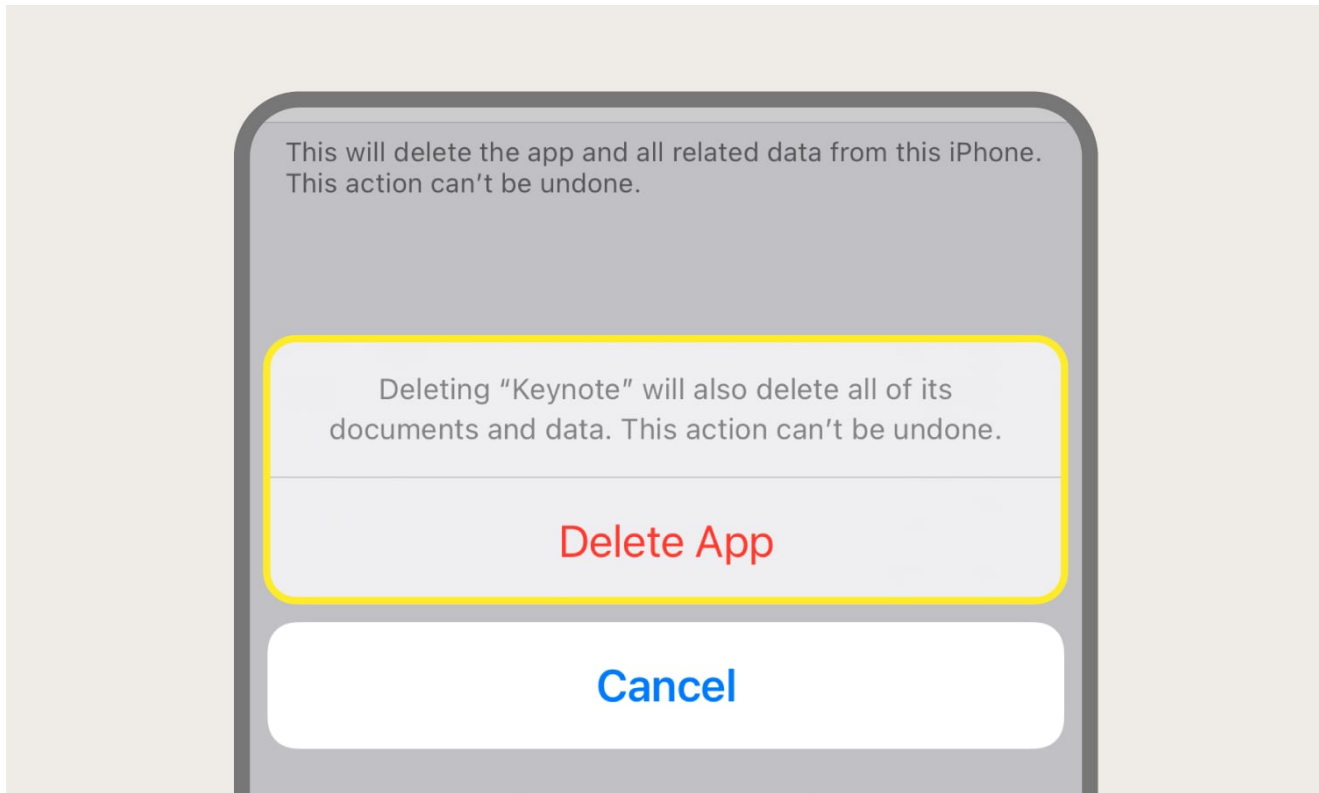
1. From your Applications tab, select "Settings."
2. Click "Apps & notifications." You might have to click "See all XXX apps" to review all your downloaded applications.
3. Select the unwanted app from the list (we're using the preinstalled Android Auto app as an example).
4. Click "Disable."

## How to remove bloatware from iOS

---







Like Android devices, bloatware on iOS devices often comes in the form of unwanted apps. Follow these steps to delete them for good.

1. Click your Settings icon, then scroll down and click “General.”
2. Select “iPhone Storage.”
3. Select the unwanted app (we’re using the preinstalled Keynote app as an example).
4. Select “Delete App.”
5. To confirm, click “Delete App” again.

## How to avoid bloatware

---

Avoiding bloatware can be much easier than uninstalling it. Consider the following methods to debloat your devices from the start.

### Purchase a bloatware-free device

---

As with all things in life, you get what you pay for — and bloatware-free devices can come with a higher price tag. Researching manufacturers can help you find brands that have vowed to avoid bloatware.

Still, even manufacturers don’t always know if their devices are bloatware-free if malicious actors are installing bloatware on them. For this reason, you could also purchase an unlocked device that’s not tied to a specific carrier. This, however, means you’re purchasing a device that might not be under warranty and might not have security measures in place.

## Take inventory of your software

---

Another best practice is to take stock of all the existing software, apps, and programs on your devices right when you unbox them. Attempt to uninstall anything you don't recognize or feel is unnecessary before downloading your preferred programs. You can use bloatware uninstallers to determine what is worth avoiding.

## Be proactive

---

Be diligent about fighting bloatware by removing any questionable apps or programs right when they pop up on our devices. In addition, only download software from known sources and consider leveraging antivirus software or anti-adware tools to monitor bloatware for you.

Remember, bloatware is a subjective term. This means you only need to rid your device of it as you see fit. What's most important is recognizing that it exists and proactively decluttering your devices to avoid the potential cyberthreats that stem from unwanted programs.

*\* The inclusion of websites, apps, brands, service providers, or links does not imply endorsement or support of any company, product, and/or provider listed herein, nor should it be inferred that NortonLifeLock is endorsed by, sponsored by, or affiliated with such brands.*

## **Cyber threats have evolved, and so have we.**

---

Norton 360™ with LifeLock™, all-in-one, comprehensive protection against viruses, malware, identity theft, online tracking and much, much more.

**Try Norton 360 with Lifelock.**

[Learn More](#)



- Clare Stouffer

- Gen employee

Clare Stouffer, a Gen employee, is a writer and editor for the company's blogs. She covers various topics in cybersecurity.

**Editorial note:** Our articles provide educational information for you. Our offerings may not cover or protect against every type of crime, fraud, or threat we write about. Our goal is to increase awareness about Cyber Safety. Please review complete Terms during enrollment or setup. Remember that no one can prevent all identity theft or cybercrime, and that LifeLock does not monitor all transactions at all businesses. The Norton and LifeLock brands are part of Gen Digital Inc.